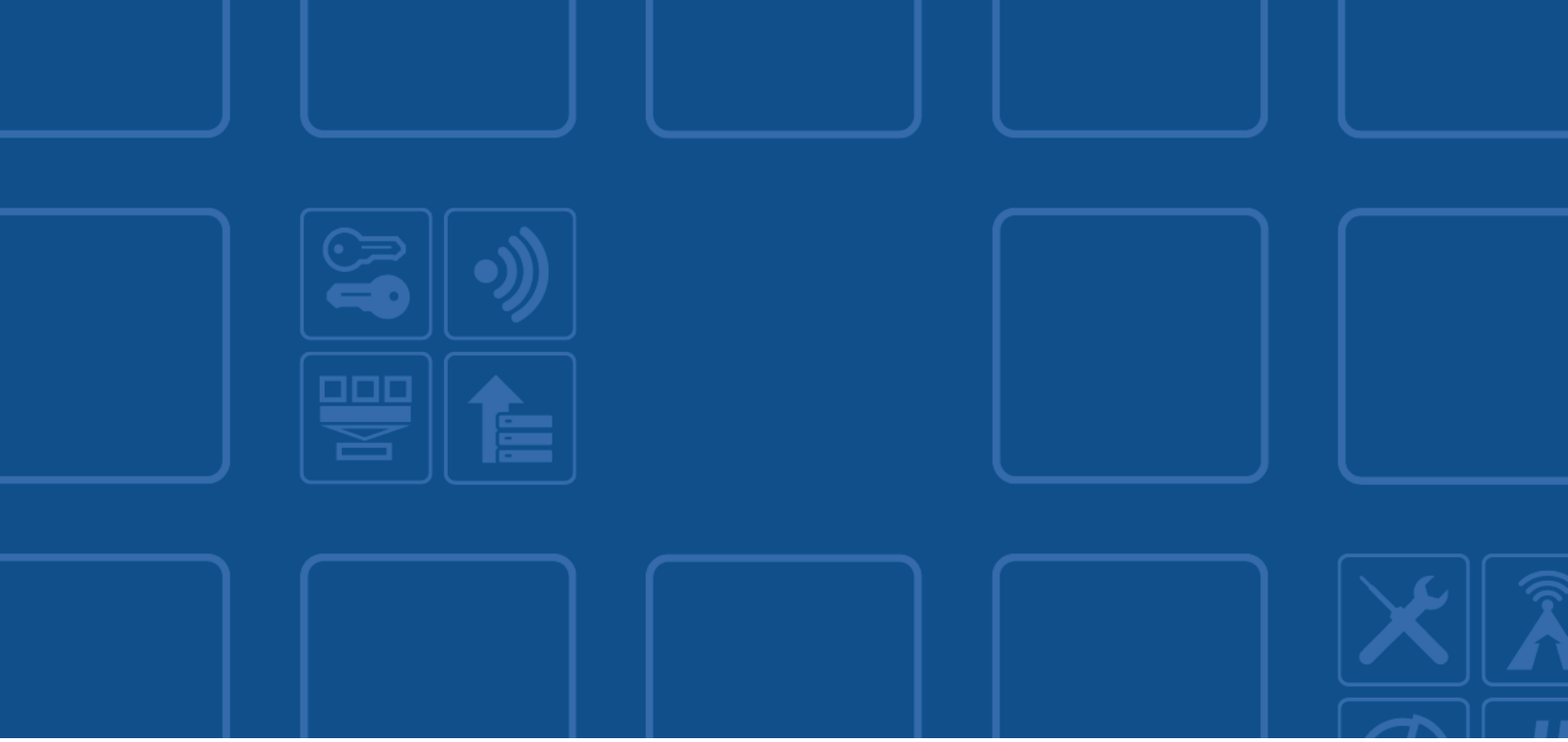
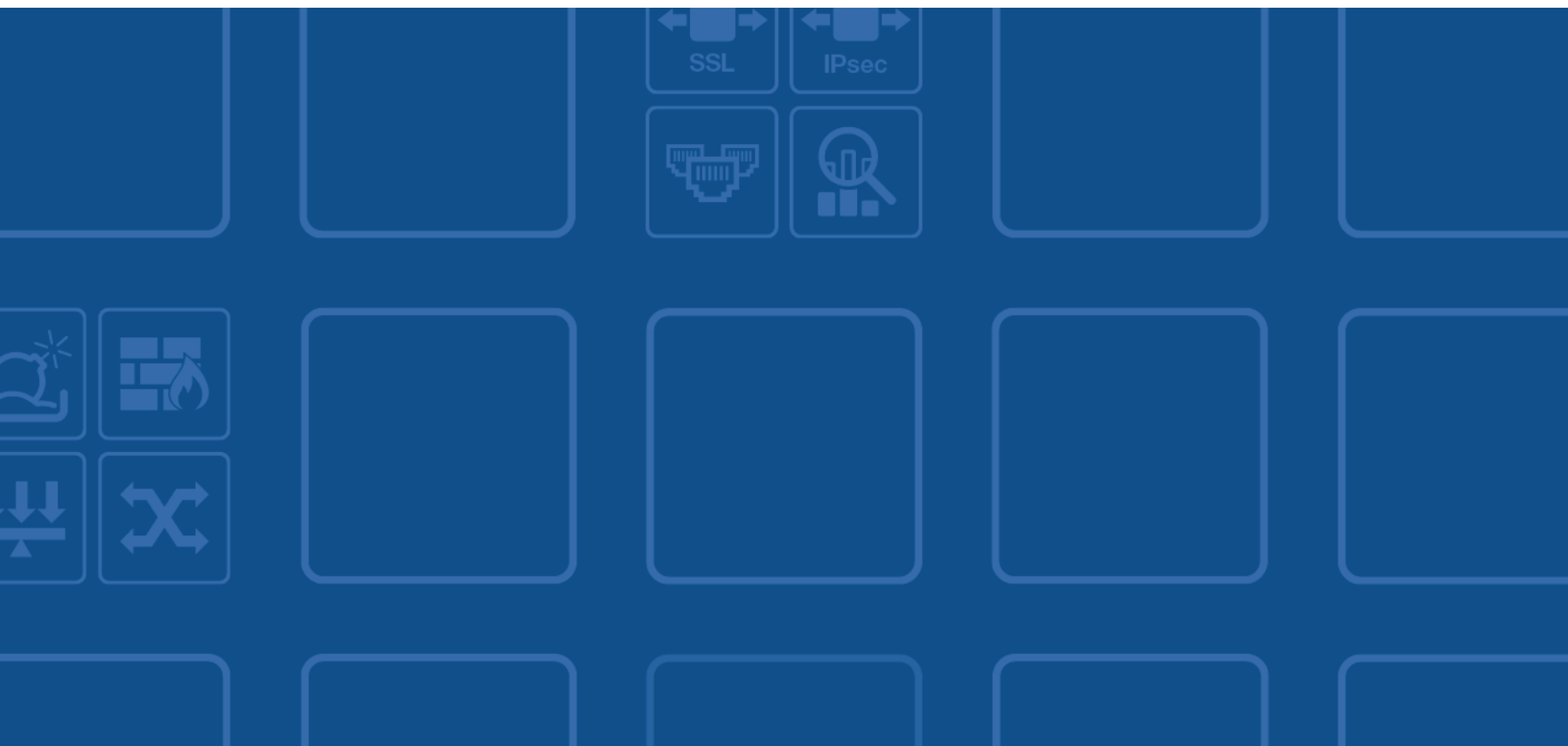


FORTINET
High Performance Network Security

FortiGate Connector for Cisco ACI - Release Notes

Version 1.3



FORTINET DOCUMENT LIBRARY

http://docs.fortinet.com

FORTINET VIDEO GUIDE

http://video.fortinet.com

FORTINET BLOG

https://blog.fortinet.com

CUSTOMER SERVICE & SUPPORT

https://support.fortinet.com

http://cookbook.fortinet.com/how-to-work-with-fortinet-support/

FORTIGATE COOKBOOK

http://cookbook.fortinet.com

FORTINET TRAINING SERVICES

http://www.fortinet.com/training

FORTIGUARD CENTER

http://www.fortiguard.com

END USER LICENSE AGREEMENT

http://www.fortinet.com/doc/legal/EULA.pdf

FEEDBACK

Email: techdocs@fortinet.com

Tuesday, August 23, 2016

Release Notes- FortiGate Connector for Cisco ACI v1.3

01-540-371310-20160505

FortiGate Connector for Cisco ACI v.1.3

Introduction

This document provides the following information for FortiGate Connector v1.3 for Cisco ACI v1.2 (2.x). This product can also refer as FortiGate Device Package for Cisco APIC.

Supported Models

FortiGate Connector for Cisco ACI v1.3 supports the following predefined models:

- FG-300D
- FG-600D
- FG-900D
- FG-1000C
- FG-1000D
- FG-1200D
- FG-1500D
- FG-3000D
- FG-3100D
- FG-3200D
- FG-3700D
- FG-VM

Unknown models

The use of FortiGate Connector can be attempted with any FortiGate model, but do so with caution. Only those listed above have been confirmed. If an unknown model of FortiGate is used, the user needs to verify port names match the real FortiGate model.

Supported Features

The FortiGate Connector for Cisco ACI supports the following functions:

Baseline features from v.1.0 to v.1.1

- Cisco ACI service insertion - software package for FortiGate device deployed to Cisco APIC, containing FortiGate models, function description, version, credentials, as a L4-L7 service.
- Enable tenant configuration to add/modify/delete L4-L7 device of FortiGate firewall service.
- Enable FortiGate deployment as both physical and virtual device (FortiGate chassis & VM).
- Support both transparent (GoThrough) and L3 (GoTo) device mode .
- Automatically create VDOM (context). One VDOM per logical device under a tenant.
- Enable FortiGate specific interface configuration: physical interface and port channel.
- Support IP address configuration on Layer 3 interfaces.
- Support subnet and service object configuration.
- Enable FortiGate firewall device to connect to endpoint groups (EPGs).
- Support IPv4 policies: match, action, network operations & security features' selection.
- Support NAT.
- Enable service graph to add/modify/delete FortiGate firewall service node
- Multiple interfaces can be added in the same device
- Single logical port can be shared in the same EPG for multiple service graphs
- Single VDOM can be used in multiple service graphs

Additional features added in v1.2

- High Availability (Active-Standby Mode)
- OSPF based routing configuration in the L3 (GoTo) mode
- Support for logging and error reporting of Fortigate as a L4-L7 device
- Automatically create VDOM based on APIC virtual device ID
- Policy enable/disable support
- Enable/Disable DDoS features
- Enable/Disable UTM Security Profiles

Additional features added in v1.3

- IPv6 Policy Configuration
- Firewall Port Forwarding (Destination NAT)
- APIC Dynamic EPG Notification
- Monitor Fortigate Devices (Health) Status
- Fortigate Device Packet Statistics on physical port

Special Notices

Predefined keywords

Do not modify the predefined key words used by FortiGate.

Custom Addresses and Services character limitations

The name fields of Firewall Addresses and Services should not include spaces or special characters.

VDOM name limitations

Beginning with FortiGate Connector v1.2, VDOM name is no longer a configurable option due to design recommendation from Cisco. The VDOM name will be the virtual device ID. After a service graph is deployed, a virtual Device ID is randomly assigned by Cisco APIC and that will be the VDOM name appears on Fortigate.

Rule ID sequence and Policy Name

Rule ID with lowest number will get processed and listed first on the FortiGate. In addition, if deploying multiple service graphs shared with same virtual device, please ensure Rule IDs and Policy Names are unique otherwise, they will override each other.

OSPF Configuration

User doesn't need to perform any OSPF parameter configuration except Router ID configured in Router Configurations under L4-L7 services. The recommendation from Cisco is that user creates OSPF Configuration on L3OUTs which is the corresponding interface configuration along with all OSPF parameters to the FortiGate on APIC. During the Service Graph deployment, FortiGate Connector device package will extract the OSPF parameters from APIC and then program the corresponding OSPF configurations on FortiGate.

Transparent Mode and NAT Mode Configuration

Beginning with FortiGate FortiConnector v1.2, the device package no longer has the option to select VDOM mode. When Go-Through mode is selected, interface ip address field must be in default setting; when "GoTo" mode is selected, interface ip addresses must be configured with valid ip address and network mask.

Change of VRF mapping After Service Graph Deployed

We uncovered a design issue for specific scenario where user changed VRF mapping after the service graph deployed which caused out of sync behavior between Cisco APIC and FortiGate.

We are actively working with Cisco to address this issue. At the meantime, the work around will be to remove the service graph, change the VRF mapping and then re-deploy the service graph. This behavior was observed on APIC version 1.2(3c) but not in 1.3(1g).

Static Route Sequence Number

For Static Route Sequence Number of 0 (default value), Device Package will ignore static route programming. Otherwise, Device Package will program any entry in the Static Route fields when Sequence Number is greater than 0.

Faults Report

When Device Package returned fault(s) to Cisco ACI due to various reasons, the fault message(s) will show up in Cisco ACI System level instead of Tenant level. However, you will still see the fault from the `debug.log` file.

Device Interface Name change

Beginning with FortiGate Connector v1.3, the ***Device Interface Name*** is allowed to be changed.

Product Integration and Support

Fortinet Products

This Version of FortiConnector for Cisco ACI is compatible with the following firmware:

- FortiOS 5.4.0 and above

Cisco Environment

This Version of FortiConnector for Cisco ACI is supported by the following Cisco ACI environments:

- Cisco ACI v1.2 (3h) or later

Known Issues

The following issues have been identified in version 1.3. For inquires about a particular bug or to report a bug, please contact Customer Service & Support.

Bug ID	Description
0380064	Enhancement for Cisco to resize Window Size for Functional Profile and Service Graph Template.
0380069	When Service Graph generated Fault, the Fault message will display at System Level instead of Tenant Level. Cisco has been notified on this issue.
0380071	Enhancement to Cisco to allow hide full path to objects with drop down menu selection.

Known issues from previous versions not listed here have been resolved.

Limitations

There are limitations to the FortiGate Connector and FortiGate combination. Some of these will be limitations of what the FortiGates can do in the environment. Some of these limitations will be what the FortiGate Connector can do. The limitations are:

- Dynamical routing protocol BGP is not supported.
- Proxy Policy is not supported.
- SSL/SSH Inspection is not supported.
- Administrator profile for limited access of different administrator accounts is not supported.
- Firewall logging: allowed traffic, security events, all sessions, etc is not supported.
- Firewall packet capture is not supported.
- Firewall with FortiGuard DDNS is not supported.

FORTINET®

High Performance Network Security